

Tecniche e tipologie di attacco ai sistemi ICT

Un'anticipazione dei dati dell'Osservatorio sugli Attacchi Informatici in Italia (OAI)

Marco R.A. Bozzetti
Ceo Malabo Srl, Partner Gealab Srl,
Comitato Tecnico-Scientifico FTI,
Consiglio Direttivo FidaInform e AIPSI

Pieraugusto Pozzi
Direttore FTI (Forum per la Tecnologia dell'Informazione)



Obiiettivo principale dell'Osservatorio OAI è quello di fornire concrete indicazioni sugli attacchi ai sistemi informatici delle Aziende e degli Enti Pubblici italiani che possano essere di riferimento nazionale, autorevole e indipendente, per l'analisi del rischio. Per raccogliere dagli operatori i dati da elaborare si è ripreso ed ampliata la metodologia di analisi che era stata definita nell'Osservatorio sulla Criminalità ICT (OCI), realizzato dal 1997 al 2004 da FTI-Sicurforum¹. Dal 2008, OAI è coordinato da Marco Bozzetti, socio fondatore e componente del Comitato Scientifico di FTI ed è realizzato con il supporto organizzativo ed economico di Soiel International con il patrocinio di FTI, FidaInform, ClubTI di Milano, AIPSA, AIPSI, Assintel, Aused, Inforav, itSMF e con la collaborazione della Polizia delle Comunicazioni e i suoi risultati sono stati pubblicati anche on line nei siti riportati in nota². La raccolta dati viene svolta tramite un questionario online indirizzato ai CIO (Chief Information Officer), CSO (Chief Security Officer) e CISO (Chief Information Security Officer) di più di mille aziende ed enti pub-

blici centrali e locali. Il compilatore può rimanere anonimo, e per ovvi motivi di riservatezza non sono richieste informazioni di dettaglio sull'azienda/ente e sui sistemi informativi, così da non consentire di risalire alla stessa. Il lavoro di OAI consente quindi di favorire lo sviluppo di sensibilità e cultura in materia di sicurezza delle informazioni e delle comunicazioni soprattutto a li-

1 La presentazione dei dati OCI, corredata da contributi di esperti riconosciuti a livello nazionale ed internazionale, è stata oggetto di tre volumi pubblicati da Franco Angeli nel 1997 (Osservatorio sulla criminalità informatica – Rapporto 1997), nel 2000 (M. Bozzetti, P. Pozzi, Cyberwar o sicurezza? Secondo Osservatorio Criminalità ICT) e nel 2004 (Pieraugusto Pozzi, Roberto Masotti, Marco Bozzetti, Crimine virtuale, minaccia reale. ICT Security: politiche e strumenti di prevenzione. Terzo Rapporto Sicurezza ICT).

2 Il primo Rapporto 2009 OAI è stato stampato da Soiel International in edizione limitata, ed è disponibile on line gratuitamente sul sito dell'autore www.malaboadvisoring.it, insieme agli articoli mensili della Rubrica OAI pubblicati sulla rivista Office Automation.



vello dei “non tecnici”, tipicamente i manager e i vertici dell’organizzazione che decidono e stabiliscono i budget.

Infatti, l’elemento fondamentale per l’analisi dei rischi ai quali i sistemi ICT sono sottoposti, è la disponibilità di dati quantitativi e qualitativi sugli attacchi che si sono verificati, su come siano stati rilevati, sulle conseguenze operative ed economiche che abbiano determinato. In sintesi sulla tipologia e sull’ampiezza del fenomeno. Proprio per colmare tale vuoto informativo nasce OAI, in analogia con la rilevazione compiuta annualmente negli Stati Uniti dal CSI, Computer Security Institute..

LA CLASSIFICAZIONE DEGLI ATTACCHI

Come è noto, la sicurezza ICT è definita come la protezione dei requisiti di integrità, disponibilità e confidenzialità delle informazioni trattate, ossia acquisite, comunicate, archiviate, processate e, per le informazioni e i sistemi connessi in rete, le esigenze di sicurezza includono anche autenticità, ossia la certezza da parte del destinatario

dell’identità del mittente e non ripudio, ossia il mittente o il destinatario di un messaggio non ne possono negare l’invio o la ricezione.

Si verifica un attacco contro un sistema ICT quando è violato almeno uno di questi requisiti sopra esposti. In particolare, OAI è indirizzato a rilevare azioni deliberate e intenzionali rivolte contro i sistemi ICT e non a misurare i rischi cui i sistemi sono sottoposti per il loro cattivo funzionamento, per un loro maldestro uso o per fenomeni accidentali esterni, quali calamità naturali o incidenti (allagamenti, terremoti, incendi, black-out, etc.). Gli attacchi intenzionali possono provenire dall’esterno dell’organizzazione considerata, tipicamente da Internet e/o da accessi remoti, o dall’interno dell’organizzazione stessa. La tassonomia degli attacchi usata per raccogliere i dati nella Tabella1: volutamente tale tassonomia è schematica per semplicità espositiva e rapidità di compilazione. Oltre al rilevamento degli attacchi subiti, il questionario richiede al compilatore, che può rimanere totalmente anonimo ed al quale si assicura comunque la totale riservatezza dei dati forniti, ulteriori informazioni sulle presunte motivazioni dell’attaccante, sulla stima dei danni subiti, sulle misure di protezione e prevenzione in essere e previste nel futuro, dal tipo di organizzazione per la sicurezza esistente e sugli attacchi più temuti nel futuro.

LE CARATTERISTICHE DEL CAMPIONE

L’ultima rilevazione OAI ha riguardato gli attacchi subiti nel 2009 e nel 1° quadrimestre 2010. Al questionario hanno risposto più di 120 enti ed aziende italiane, appartenenti ai vari settori merceologici come dettagliato nelle Fig. 2a, 2b e 2c. La figura 2a evidenzia come i settori dell’ambito finanziario (banche, assicurazioni) e della Pubblica Amministrazione, sia locale che centrale, abbiano risposto in maniera molto esigua, nonostante le innumerevoli sollecitazioni sia in posta elettronica che telefoniche. Le motivazioni riguardano sia il poco tempo disponibile da parte dei responsabili ICT e/o della sicurezza a rispondere, sia le autorizzazioni necessarie all’interno delle strutture per fornire questi tipi di informazioni sia infine la non volontà o la non capacità di fornirli. La fig.2b illustra le dimensioni (per numero di dipendenti) degli enti che formano il campione, che risulta ben bilanciato tra piccole, medie e grandi. La figura 2c mostra il ruolo nella struttura di chi ha risposto al questionario: la maggior parte dei rispondenti sono responsabili dei sistemi informativi e della sicurezza informatica ed è interessante evidenziare che un numero non trascurabile di rispondenti sono persone del

vertice aziendale: presidente o amministratore delegato, specie per le strutture piccole. Come evidenziato nella fig. 2, il campione considerato per il Rapporto OAI non è predefinito e selezionato statisticamente, ma risulta dall'insieme delle risposte "volontarie". Il numero e la ripartizione dei rispondenti, per tipo di settore e per dimensioni, fornisce però valide ed interessanti indicazioni - che nessun altro rapporto fornisce specificatamente per l'Italia - sulle effettive tendenze degli attacchi ICT subiti.

LA SITUAZIONE DEGLI ATTACCHI IN ITALIA

La fig. 3 rappresenta la sintesi dei diversi Rapporti OAI dal 2007 al 2010 in termini di quantità di attacchi rilevati in percentuale sul campione considerato. Si evidenzia come dal 2008 siano diminuiti gli attacchi rilevati e subiti, anche se è aumentata la gravità dell'attacco andato a buon fine.

La fig. 4 dettaglia la tipologia degli attacchi subiti nell'ultimo periodo considerato.

La Tabella 2 schematizza le principali misure di prevenzione e di protezione in essere: dai dati rilevati emerge come il campione considerato sia mediamente "ben protetto" in termini di stru-

menti, anche se gli aspetti organizzativi e di policy sono ancora limitati alle grandi organizzazioni.

PRIME CONCLUSIONI

Premesso che i dati presentati rappresentano una prima e limitata anticipazione dei risultati dell'ultimo Rapporto OAI che verrà reso disponibile entro il primo semestre 2011 nei siti degli enti patrocinatori e in quello del coordinatore, la tendenza più evidente indica, da un lato, come si stiano rafforzando e diffondendo gli strumenti e le misure di sicurezza, tanti che il numero di attacchi subiti si sta riducendo, ma dall'altro come gli attacchi siano sempre più sofisticati e pericolosi.

Gli attacchi si basano prevalentemente:

a) sulle vulnerabilità del software di base e applicativo, in base alle quali vengono realizzati i codici maligni. Le vulnerabilità sono in crescita, talvolta non risolte dai fornitori e spesso non sistemate con le apposite patch dagli utenti. Alcuni dati nel 2010:

- il numero max di vulnerabilità divulgate: 8562 (+27% rispetto al 2009);
- il 44% delle vulnerabilità non ha avuto patch di correzione;

1. Attacchi fisici, quali sabotaggi e vandalismi, con distruzione di risorse informatiche e/o di risorse a supporto (es. UPS, alimentatori, condizionatori, ecc.) a livello centrale o periferico .
2. Furto di apparati informatici facilmente nascondibili e trasportabili contenenti dati (unità di rete, Laptop, hard disk, floppy, nastri, Chiavette USB, ecc.)
3. Furto di informazioni e loro uso illegale sia da dispositivi mobili (palmari, cellulari, laptop) sia da tutte le altre risorse ICT
4. Frodi tramite uso improprio o manipolazioni non autorizzate ed illegali del software applicativo (ad esempio utilizzo di software pirata, copie illegali di applicazioni, ecc.)
5. Attacchi di Social Engineering e di Phishing per tentare di ottenere con l'inganno (via telefono, e-mail, chat, ecc.) informazioni riservate quali credenziali di accesso, identità digitale, ecc.
6. Ricatti sulla continuità operativa e sull'integrità dei dati del sistema informativo (es: se non paghi attacco il sistema e ti procuro danni, normalmente con dimostrazione delle capacità di attacco e di danno conseguente ...)
7. Accesso a e uso non autorizzato degli elaboratori, delle applicazioni supportate e delle relative informazioni
8. Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.
9. Modifiche non autorizzate ai dati e alle informazioni
10. Utilizzo vulnerabilità del codice software, sia a livello di posto di lavoro che di server: tipici esempi back-door aperte, SQL injection, buffer overflow, ecc.
11. Utilizzo codici maligni (malware) di varia natura, quali virus, Trojan horses, Rootkit, bots , exploits, sia a livello di posto di lavoro che di server.
12. Saturazione risorse informatiche e di telecomunicazione: oltre a DoS (Denial of Service), DDoS (Distributed Denial of Service) e Botnet, si includono in questa classe anche mail bombing, spamming, catene di S. Antonio informatiche, ecc.
13. Attacchi alle reti, fisse o wireless, e ai DNS, Domain Name System

Tabella 1: OAI, tassonomia attacchi rilevati

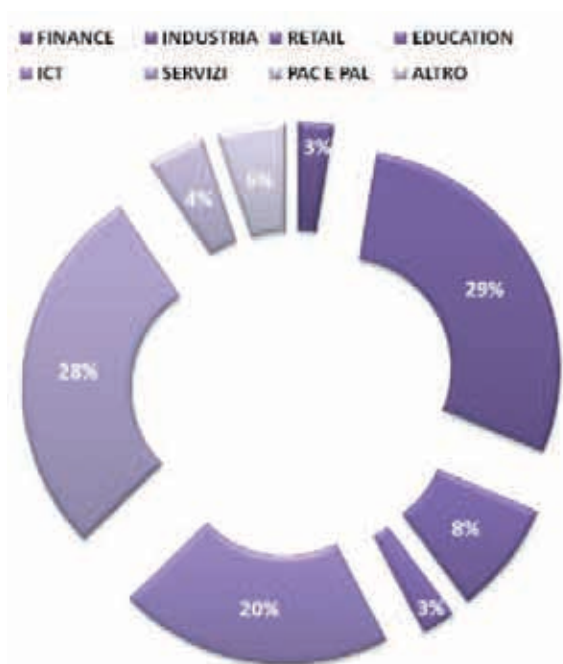


Figura 2a: settore merceologico OAI 2011

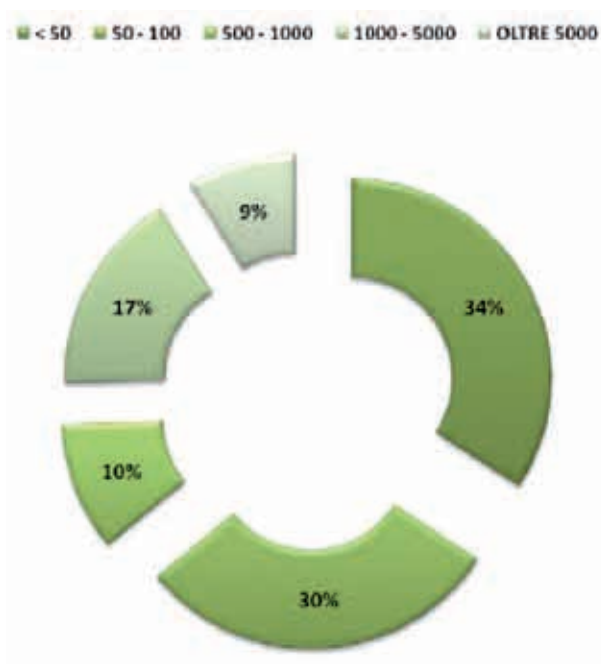


Figura 2b: tipologia dimensionale OAI 2011

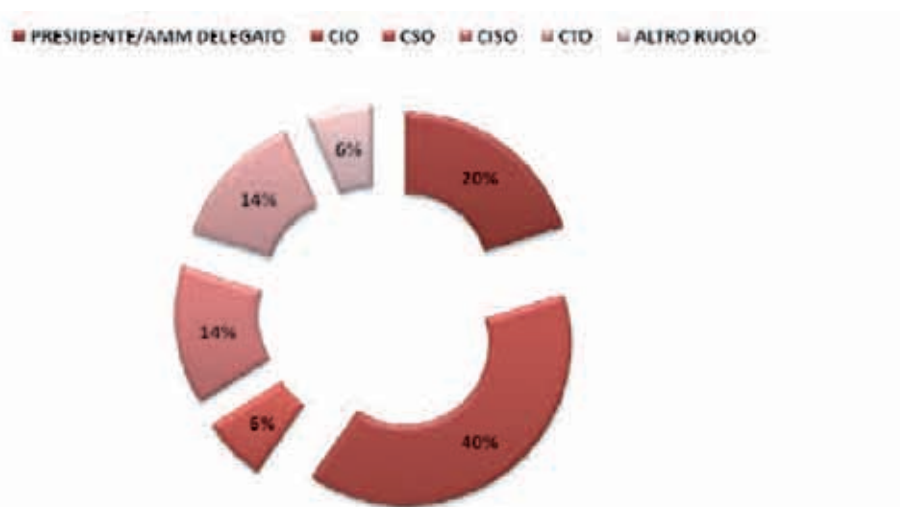


Figura 2c: ruolo aziendale OAI 2011

- con la virtualizzazione si sono introdotte 373 nuove vulnerabilità
- a) sul social engineering, sfruttando disponibilità e in taluni casi la disattenzione e/o ingenuità degli utenti finali. La diffusione dei social network, quali Facebook, YouTube, LinkedIn, anche a livello aziendale, oltre che della posta elettronica, dei motori di ricerca, dell'uso di sempre più potenti chiavette USB, e degli strumenti collaborativi apre crescenti possibilità di carpire facilmente informazioni riservate con le quali svolgere attacchi e compiere frodi

sia a livello del singolo che delle aziende ed enti.

La maggior parte degli attacchi sono ormai finalizzati a frodi e a compiere significativi danni sull'attaccato. La sicurezza dei sistemi informativi assume un ruolo crescente anche per le piccole e medie organizzazioni, che devono imparare a prevenire in maniera sistematica e continua. Di qui l'importanza di poter disporre dei dati raccolti ed elaborati da OAI sul reale stato dell'arte in Italia e di quanto, sotto il profilo delle scelte aziendali e organizzative, sia importante pensare

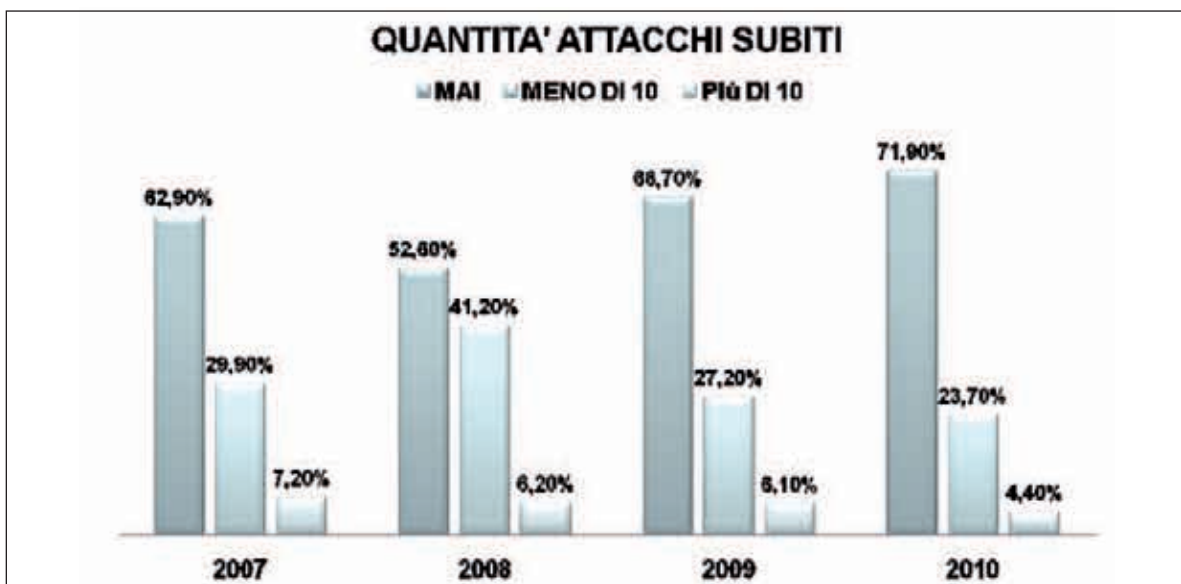


Figura 3: OAI, numero attacchi dal 2007 al 2010



Figura 4: OAI, tipologia attacchi subiti

Tabella 2: OAI, misure di prevenzione e protezione in essere

| | |
|---|--------|
| CONTROMISURE FISICHE | |
| CONTROMISURE LOGICHE | 93,20% |
| CONTROMISURE LOGICHE (M.A.) | |
| Controlli di perimetri | 94,80% |
| CONTROMISURE LOGICHE (PROTEZIONE RETI) | |
| Firewall (perimetria e logica) e IDS/IPS | 90,20% |
| CONTROMISURE LOGICHE (PROTEZIONE RETI) | |
| Firewall e IDS | 93,20% |
| CONTROMISURE LOGICHE (PROTEZIONE SISTEMI) | |
| Antivirus | 100% |
| CONTROMISURE LOGICHE (PROTEZIONE APPLICATIVE) | |
| Strumenti di backup e recovery | 96,20% |
| CONTROMISURE ORGANIZZATIVE | |
| Security Awareness (ET) | 91,90% |
| Controlli di sicurezza (ET) | 91,20% |

alla sicurezza globale ICT come ad un aspetto fondamentale della politica di continuità operativa e di salvaguardia del patrimonio operativo, soprattutto in tempo di crisi come quelli attuali,

nei quali le risorse anche economiche per la sicurezza ICT non devono essere oggetto di semplice riduzione, ma piuttosto razionalizzate ed ottimizzate. ■